ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

# Θέμα Διπλωματικής Εργασίας

# Μελέτη Αλγορίθμων Κρυπτογραφίας Ελλειπτικών Καμπυλών και Υλοποίηση σε Υλικό του Αλγορίθμου Karatsuba
# Study of Elliptic Curve Cryptography Algorithms and Material Implementation of the Karatsuba Algorithm

**Επιβλέπων: Δρ. Μηνάς Δασυγένης (** mdasyg **(at)** ieee .org**) -http://arch.icte.uowm.gr**

Η επικοινωνία μέσω δημόσιων καναλιών κάνει την ανάγκη για χρήση της κρυπτογραφίας επιτακτική. Το πρόβλημα όμως που δημιουργείται είναι ότι όλες οι περιορισμένες πλατφόρμες υστερούν στην υπολογιστική ισχύ τους και αδυνατούν στην επεξεργασία πολύπλοκων αλγορίθμων. Συνήθως αυτό συμβαίνει λόγω ανεπαρκούς μνήμης, με αποτέλεσμα οι αλγόριθμοι των "συμβατικών" κρυπτοσυστημάτων να είναι αδύνατον να πραγματοποιηθούν. Αντίθετα για να πραγματοποιηθούν οι αλγόριθμοι που χρησιμοποιούν οι ελλειπτικές καμπύλες, χρειάζονται αρκετά μικρότερη μνήμη. Τα κλειδιά που χρησιμοποιούνται είναι αρκετά μικρότερα, και επομένως απαιτείται μικρότερη υπολογιστική ισχύ. Επίσης, οι πράξεις που εκτελούνται είναι υπολογιστικά ευκολότερες και πραγματοποιούνται πολύ ποιο γρήγορα .

Πρόκειται για ένα σύγχρονο πεδίο με έντονο ερευνητικό ενδιαφέρον καθώς οι κρυπτογραφικοί αλγόριθμοι που βασίζονται στη θεωρία των ελλειπτικών καμπυλών προσφέρουν το ίδιο επίπεδο ασφάλειας με τον αλγόριθμο κρυπτογραφίας RSA αλλά με πολύ μικρότερο μήκος κλειδιών που ανταλλάσσονται μεταξύ των χρηστών.

Στην εργασία αυτή θα προηγηθεί η βιβλιογραφική έρευνα του αντικειμένου και ο εντοπισμός των προβλημάτων και η διερεύνηση των μέχρι τώρα λύσεων. Θα συνεχίσουμε με τη μελέτη αλγορίθμων κρυπτογραφίας ελλειπτικών καμπυλών, τους οποίους συναντάμε στη διεθνή βιβλιογραφία. Για τον σκοπό της εργασίας θα αξιοποιηθεί ο αλγόριθμος Karatsuba καθώς και σειριακή υλοποίηση του, για εξοικονόμηση υλικού. Ο αλγόριθμος Karatsuba είναι ένας αλγόριθμος γρήγορου πολλαπλασιασμού. Ανακαλύφθηκε από τον Anatoly Karatsuba το 1960 και δημοσιεύθηκε το 1962. Μειώνει τον πολλαπλασιασμό δύο n-ψηφίων αριθμών στο μέγιστο, χρησιμοποιώντας μονοψήφιους πολλαπλασιασμούς. Επομένως, είναι ταχύτερος από τον κλασσικό αλγόριθμο, ο οποίος απαιτεί $n^2$ μονοψήφια στοιχεία. Επίσης, θα μελετηθούν ο αλγόριθμος Toom-Cook που είναι μια ταχύτερη γενίκευση της μεθόδου του Karatsuba και ο αλγόριθμος Schönhage-Strassen που είναι ακόμα πιο γρήγορος, για αρκετά μεγάλο n. Η υλοποίηση του αλγορίθμου θα γίνει σε πλατφόρμες FPGA με χρήση γλώσσας περιγραφής υλικού VHDL.

**Απαιτήσεις:** Κρυπτογραφικοί αλγόριθμοι, Προγραμματισμός VHDL, Ψηφιακή σχεδίαση, Αρχιτεκτονική FPGA.

**Πλεονεκτήματα:** Με την παρούσα διπλωματική εργασία ο φοιτητής θα αποκομίσει καλή γνώση σχεδιασμού ψηφιακών συστημάτων, προγραμματισμού με VHDL και την εμπειρία της υλοποίησης σύγχρονων κρυπτογραφικών εφαρμογών για την προστασία της πληροφορίας σε επίπεδο υλικού.

**Ενδεικτική βιβλιογραφία**

1. Gayoso Martínez, V., Hernández Encinas, L., & Sánchez Ávila, C. (2010). A survey of the elliptic curve integrated encryption scheme.
2. Eyupoglu, C. (2015). Performance Analysis of Karatsuba Multiplication Algorithm for Different Bit Lengths. Procedia-Social and Behavioral Sciences, 195, 1860-1864.